Amendments to the Claims

1. (currently amended) A method comprising:

receiving, at a BIOS, a message from an authorized party, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor;

authenticating the message; and

when the message has been successfully authenticated,

controlling a state of an optional feature of a system resource, using the BIOS, according to the message, wherein the message comprises information to determine the optional feature, and wherein the message further comprises a digital signature, and

when the message fails the authenticating, then discarding the message.

2. (original) The method of claim 1 further comprising verifying an identifier in the message against a unique system identifier of the system.

3. (original) The method of claim 1 further comprising writing the message into a secure non-volatile location.

4. (original) The method of claim 3 wherein the secure non-volatile location comprises a remote storage.

5. (previously presented) The method of claim 1 further comprising splicing the content of the message into an execution path of the BIOS, wherein the splicing comprises at least one of modifying the BIOS or erasing a portion of the BIOS, in response to the message.

6. (previously presented) The method of claim 1 further comprising loading and executing content of the message using the BIOS at run-time, wherein the message is received via a network transmission.

PAGE 6/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY

7. (previously presented) The method of claim 1 further comprising updating a feature set of the system BIOS according to the message.

8. (currently amended) A system comprising:

a system resource having controllable optional features; and

a non-volatile memory that stores a BIOS, the BIOS being adapted to receive a secure message from an authorized party for controlling at least one of the optional features, wherein the secure message comprises information to determine the at least one of the optional features, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor, and wherein the system is to boot without enabling the at least one optional feature when the secure message is not received from the authorized party.

9. (previously presented) The system of claim 8 further comprising a write-once non-volatile unit for storing a public key accessible by the BIOS.

10. (previously presented) The system of claim 8 wherein the BIOS includes authentication circuitry for authenticating the secure message with a public key.

11. (previously presented) The system of claim 8 further comprising a write-once non-volatile unit for storing a unique system identifier accessible by the BIOS.

12. (previously presented) The system of claim 8 wherein the BIOS also includes verification circuitry for verifying an identifier in the message against a unique system identifier.

13. (previously presented) The system of claim 8 further comprising a secure non-volatile location for storing at least one of the optional features to be enabled, the location being readable and writable by the BIOS.

PAGE 7/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY

14. (previously presented) The system of claim 13 wherein the location comprises a remote storage.

15. (previously presented) The system of claim 8 wherein the BIOS also includes a feature set that is updated according to content of the secure non-volatile storage.

16. (previously presented) The system of claim 8 wherein the BIOS loads and executes the content of the message at run-time, wherein the message is received via a network transmission.

17. (currently amended) A computer program product residing on a computer readable medium comprising instructions for causing a computer to:

receive, at a BIOS, a message from an authorized party, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor;

authenticate the message; and

when the message has been successfully authenticated, control a state of a feature of a system resource, using the BIOS, according to the message, wherein the message comprises information to determine the state of a feature of a system resource, and

when the message fails the authentication, then discard the message.

18. (previously presented) The computer program product of claim 17 further comprising instructions for causing a computer to verify an identifier in the message against a unique system identifier of the system.

19. (previously presented) The computer program product of claim 17, further comprising instructions for causing a computer to write the message into a secure non-volatile location.

PAGE 8/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY

20. (previously presented) The computer program product of claim 19 wherein the secure non-volatile location comprises a remote storage.

21. (previously presented) The computer program product of claim 17 further comprising instructions for causing a computer to splice the content of the message into an execution path of the BIOS.

22. (previously presented) The computer program product of claim 17 further comprising instructions for causing a computer to load and execute the content of the message at the BIOS at run-time, wherein the message is received via a network transmission.

23. (previously presented) The computer program product of claim 17 further comprising instructions for causing a computer to update a feature set of the system BIOS according to the message.

24. (currently amended) A method comprising:

when a message from an authorized party is received at a BIOS of a system:

verifying an identifier in the message against a unique system identifier of the system,

authenticating the message, and

controlling a state of an optional feature of a system resource, using the BIOS upon booting the system, according to the message, wherein the message comprises information to determine the optional feature, and wherein the message further comprises a digital signature; and

when a message from an authorized party is not received at a BIOS:

booting the system ~~in a default state~~ without optional features.

25. (previously presented) The method of claim 24, further comprising splicing the content of the message into an execution path of the BIOS, wherein the splicing comprises at least one of modifying the BIOS or erasing a portion of the BIOS, in response to the message.

PAGE 9/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY

26. (previously presented) The method of claim 24, further comprising loading and executing content of the message using the BIOS at run-time, wherein the message is received via a network transmission.

27. (currently amended) A system comprising:

a system resource having controllable optional features, wherein the system resource is ~~one or more of the resources~~ selected from the group of system resources consisting of storage capacity, processor redundancy, processor speed, memory, input/output devices, processors, redundant power supplies, Peripheral Component Interconnect (PCI) bus, and other elements of the system contributable to processing power;

a non-volatile memory that stores a BIOS, the BIOS to receive a secure message from an authorized party for controlling at least one of the optional features, wherein the secure message comprises information to determine the at least one of the optional features; and

an authenticator to decrypt, authenticate and/or verify the secure message and to discard the secure message if failure occurs during any one of decryption, authentication and verification.

28. (previously presented) The system of claim 27, wherein the secure message is to be received by the BIOS during run-time of the system.

29. (previously presented) The system of claim 28, wherein the system is to be rebooted to enable the BIOS to control the at least one of the optional features according to the received secure message.

30. (previously presented) The system of claim 27, wherein the BIOS is to load and execute the content of the message at run-time, wherein the message is received via one of a network transmission and electronic mail.

31. (previously presented) The system of claim 27, wherein the secure message comprises executable code to be used as a Dynamically Loaded Library (DLL), and wherein the

PAGE 10/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY

DLL is to be stored in non-volatile storage coupled to the BIOS, and wherein the DLL is to be loaded by the BIOS at run-time.

32. (new) The system as recited in claim 8, wherein the system comprises a platform to authenticate the secure message by the BIOS without requiring an additional processor or hardware.

PAGE 11/22 * RCVD AT 3/20/2006 8:23:10 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/22 * DNIS:2738300 * CSID:1408 720 8381 * DURATION (mm-ss):06-38

BEST AVAILABLE COPY